Massimiliano Sala

28 Settembre 2019

Massimiliano Sala?

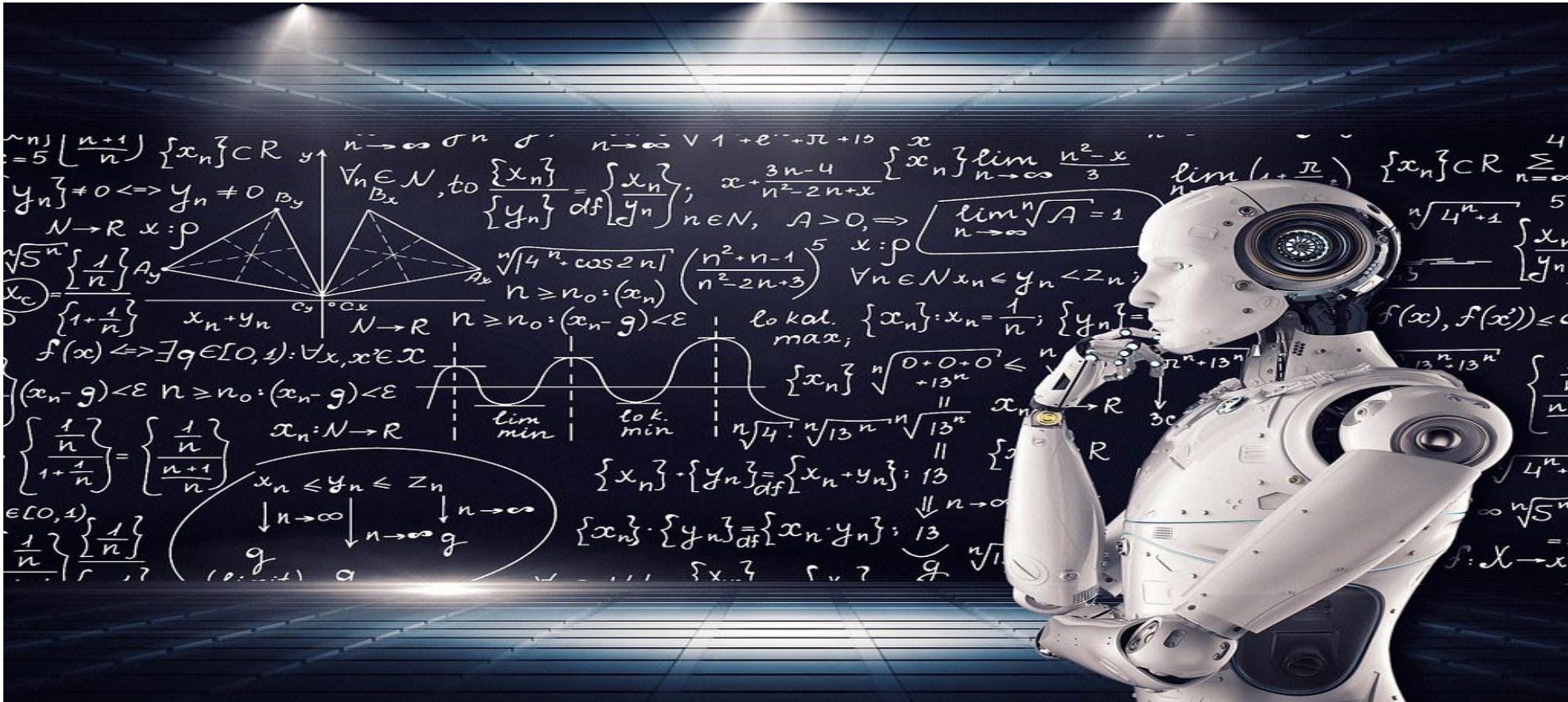
Università degli Studi di Trento

- Professore Ordinario di Algebra (**Crittografia**)
- Direttore del **CryptoLabTN**
  Laboratorio di Matematica Industriale e **Crittografia**

Associazione Crittografia De Componendis Cifris

- Acting Director

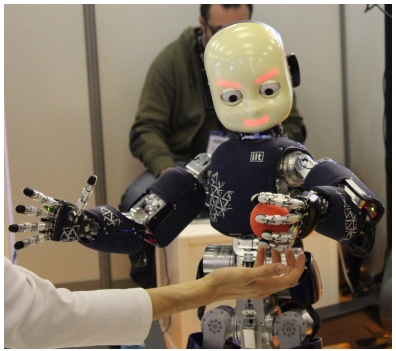
Artificial Intelligence



AI È OVUNQUE


207,513
66%
208974684_DEFENDER
2M:30S
1,520
77%
208974684_ATTACKER
DEPLOY
PREVIOUS
NEXT
RETREAT


CHECK IN
INSERT
SCAN
TYPE
LOOK
PASSPORT



COSA CI PREOCCUPA ??

1. il **robot infermiere** che tira la forchetta al malato?

2. la **tua automobile** che non ti apre la portiera perchè non riconosce il tuo viso?

3. il **sistema antimissile** che abbatte un aereo di linea ritenendolo un nemico?

COSA **DEVE** PREOCCUPARCI!

The current generation of AI systems offer tremendous benefits, but their effectiveness will be limited by the machine's inability to explain its decisions and actions to users.

(USA **DARPA** project: Explanable Artificial Intelligence)

Cyber Security

Giochi per ragazzini?

A New Pacemaker Hack Puts Malware Directly on the Device

Researchers at the Black Hat security conference will demonstrate a new pacemaker-hacking technique that can add or withhold shocks at will.

(Wired - 08/09/2018)

Giochi per ragazzini?

Ieri un'azienda mi ha telefonato: hanno

interi stabilimenti bloccati

per un'intrusione informatica

Il problema

Il mercato spinge sempre di più verso la creazione di dispositivi e programmi, interconnessi e con nuove funzionalità.

Indi -> **più vulnerabili**.

Le normative che dovrebbero tutelarci sono sempre in ritardo sull'evoluzione tecnologica e spesso disattese.

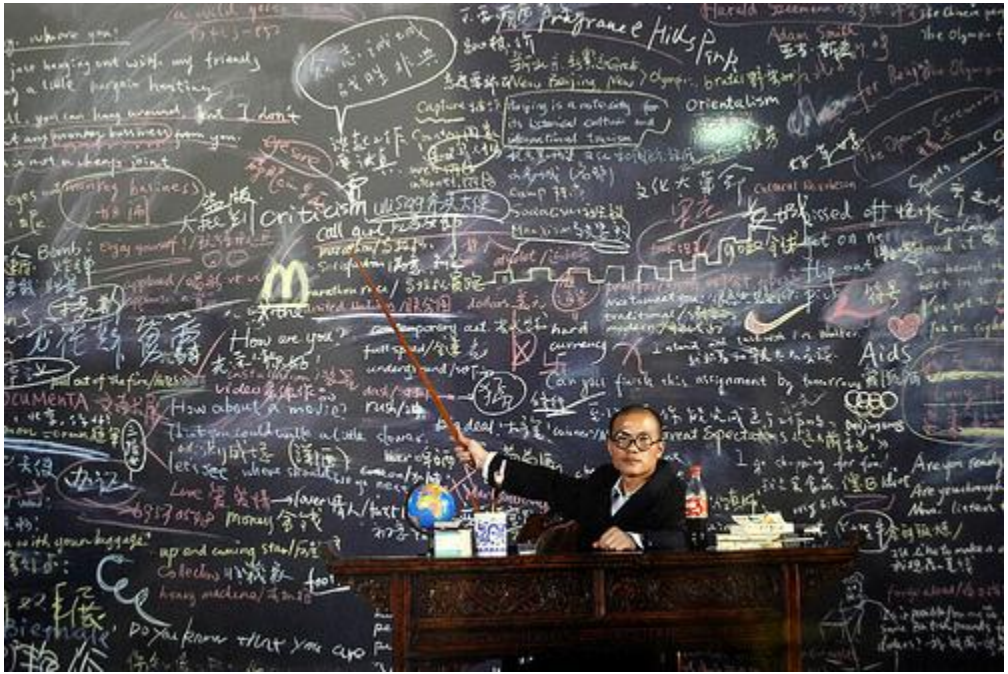
Soluzioni? Un paradosso

Non vedo soluzioni realistiche a breve, spero in:

1. crescita esponenziale della consapevolezza dei consumatori, che porti a una domanda di sicurezza

2. sforzo sulla formazione delle competenze necessarie, che sono una piccola frazione di quelle che cerca il mercato

Blockchain e Crittovalute



Blockchain: una lavagna infinita indelebile

Tutti scrivono sulla lavagna, ma la **Crittografia** garantisce:

1. l'identità digitale di chi scrive
2. l'impossibilità di alterare il contenuto
3. la natura pubblica della lavagna, conservando sicurezza

Tutti possono leggere la lavagna con fiducia**!**

Crittovalute

Grazie alla tecnologia blockchain, Satoshi inventa la prima crittovaluta: il **Bitcoin**.

Le crittovalute permettono lo scambio elettronico di denaro senza doversi avvalere di intermediari (eg. banche), riuscendo parzialmente a rimanere **anonimi**.

I don't trust people any more, I trust only Mathematics

(Satoshi Nakamoto)

Monero and friends (I)

Negli ultimi anni (2016-2018) sono state ideate nuove **Crittovalute** **specificatamente** per lo scopo di rendere non tracciabili i flussi di denaro:

1. di gran lunga la più pericolosa e più usata dal mondo criminale è **Monero**

2. molte altre esistono, tra cui Dash e ZCash

Monero and friends (II)

Monero usa **crittografia molto sofisticata** e riesce a nascondere molto bene:

1. i mittenti e i destinatari dei flussi finanziari

2. addirittura l'**importo** scambiato
   (usando una blockchain pubblica!)

Le tecniche sviluppate per l'indagine dei Bitcoin sono inutili.

De Componendis Cifris

www.decifris.it